ALERT: Point of Sale RAM scraper malware

Advances in technology have led to more sophisticated crimes by exploiting security vulnerabilities of new technologies. This is exacerbated by the fact that understanding of these technologies and their use is only by a few, while the majority of end-users are unaware. Generally speaking, following standard security practices will thwart 95% of electronic crimes such as phishing, hacking, etc. This includes using complex passwords (Sf9$fpq%f82bsS), using network firewalls, encrypted emails, etc. But the new POS RAM scraper is dangerous because the vendors are not the victims of their bad security, and you may never know where your credit card or other information was scraped from.

A look at Point of Sale RAM scraper malware and how it works

From Sophos:

A special kind of malware has been hitting the headlines recently – that which attacks the RAM of Point of Sale (PoS) systems.

Although it's been getting quite a bit of publicity recently, we actually first identified it as a threat back in December 2009 and wrote about it in an article on Naked Security entitled Will RAM scraping loosen the sky and make it fall?.

Answering that question today, it just might!

Actually, the situation isn't that bad – yet – but this malware family has definitely become more complex and far-reaching. In this article, we take a step back from the technical details and look at the evolution of PoS RAM scrapers.

What do PoS RAM scrapers do?

In a nutshell, PoS RAM scrapers steal payment data – such as credit card track one and track two data – from the RAM of PoS systems.

The payment card industry has a set of data security standards known asPCI-DSS. These standards require end-to-end encryption of sensitive payment data when it is transmitted, received or stored.

This payment data is decrypted in the PoS's RAM for processing, and the RAM is where the scraper strikes. Using regular expression searches, they harvest the clear-text payment data and send that information to rogue callhome servers.

Why do we care about PoS RAM scrapers? How does it hurt me?

I believe this malware family has a higher probability of burning a hole in your pocket compared to other prevalent malware families.

In today's plastic money economy people are carrying cash a lot less than before. Aside from a handful of stores, the majority of retailers accept debit or credit cards. Payment cards are convenient, quick, supposedly-secure, and you don't have change jingling around in your pockets.

PoS RAM scrapers target the systems which process debit and credit card transactions and steal the sensitive payment information. Your home computer might be super secure, but

there is no guarantee the PoS system at your neighborhood grocery store has the same level of security. You might end up losing your credit card data buying a candy bar!

How have PoS RAM scrapers evolved?

Sophos detects PoS RAM scraper malware under the family name *Trackr*(e.g. Troj/Trackr-Gen, Troj/Trackr-A) Other AV vendors detect this malware family with a variety of names, the most common name being *Alina*.

Some of the earliest variants of Trackr had simple functionality that worked like this:

1. Install as a service
2. Use a legitimate-looking name
3. Scan RAM for credit card track one and track two data
4. Dump the results into a text file. This text file was then probably accessed remotely or manually.

Over the years Trackr has become more industrialized, with some cosmetic changes and added bot and network functionality.

Our friends at Trustwave SpiderLabs have written two excellent articles,Alina: Casting a Shadow on PoS and Alina: Following The Shadow, about the inner workings of the Trackr family.

Till now we have observed the following types of Trackr:

- Basic version (not packed, scrapes RAM for credit card information)
- Complex version (added socially-engineered filenames, bot and network functionality)
- Installed DLL version (the DLL is registered as a service and performs the RAM scraping)
- Versions one and two packed with a commercially-available packer
- Versions one and two packed with a custom packer

Most recently, SophosLabs discovered the highly-

prevalent Citadel crimeware targeting PoS systems.

The Citadel malware uses screen captures and keylogging instead of the RAM-scraping technique used by Trackr. Citadel's focus on PoS systems demonstrates that this avenue is fast becoming a point of serious concern.

Who do PoS RAM scrapers target?

One of the earliest serious PoS RAM scraper attacks that we observed was back in November 2011 when we found that a university and several hotels had their PoS systems compromised. Later we saw varied targets including an auto dealership in Australia infected with Trackr.

To better understand the threat we gathered statistics about the various industries targeted by Trackr during the past 6 months (as observed using Sophos Live Protection):

It doesn't come as a surprise that the biggest targeted industries are:

- Retail
- Service
- Healthcare
- Food services
- Education
- Hotel and tourism

In these industries there's a high volume of credit and debit card transactions taking place, meaning they have goldmines of payment data that can be harvested.

Compromising a single PoS system (e.g. in a fast food outlet) may yield thousands of credit cards per week, cheaply – much easier to gather 10,000 credit card details from one PoS system then attempt to infect 10,000 PCs, hoping to grab the data from there.

If not protected properly, PoS systems become easy targets – a single point of failure that can affect thousands of people.

In addition to the breakdown of industries targeted, we also looked at the countries where we saw Trackr infections over the same time period:

Again, no surprises that the developed countries top this chart with the US, where credit cards are abundant, taking the #1 spot.

In fact, the Trackr infection numbers match up closely with the credit card country usage statistics published by Visa.

So how does Trackr get on a PoS system?

We have used the term PoS quite generally throughout this article. PoS is the place where a retail transaction is completed. So a PoS could be some custom hardware/software solution, a regular PC running PoS software, a credit card transaction server, or something similar.

Big box retailers and chain stores have security-hardened PoS systems, and we have not seen any major evidence of these large organizations getting compromised with Trackr.

The victims tend to be mostly small to medium sized organizations who will typically have less investment in defensive counter-measures.

Based on our analysis there were two main methods of infection:

Insider job

Someone with active knowledge of the payment processing setup installs a RAM scraper to gather data. The early Trackr samples dropped their harvested data in a plain text file

which we suspect was manually retrieved or remotely accessed.

The malware had no network functionality and we found no evidence of a top-level dropper/installer.

Phishing/Social Engineering

These are the common infection vectors with the more complex versions of Trackr. The socially engineered filenames we have observed includeTaskmgr.exe, windowsfirewall.exe, sms.exe, java.exe, win-firewall.exe, andadobeflash.exe. This suggests that the files were delivered as part of a phishing campaign, or social engineering tricks were used to infect the system.

Importantly however, Trackr is not seen regularly in the mass-spammed malware campaigns that we observe daily. Rather it is highly targeted towards a group of relevant businesses.

To conclude, it is not always a safe solution to pay for everything with cards.

Everyone should follow computer security best practices and consumers should proactively sign-up for credit monitoring services so they don’t becomes victims of credit or identity theft.

Businesses big and small need to make investments to protect their critical PoS infrastructure. Just like they wouldn’t keep their cash registers unlocked for someone to grab money out of them, PoS systems need proper protection.
